

(19)



JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **06315027 A**

(43) Date of publication of application: **08.11.94**

(51) Int. Cl.
H04L 9/06
H04L 9/14
G09C 1/00

(21) Application number: **06049081**

(22) Date of filing: **18.03.94**

(30) Priority: **23.04.93 US 93 52304**

(71) Applicant: **INTERNATL BUSINESS MACH
CORP <IBM>**

(72) Inventor: **BELLARE MIHIR
GUERIN ROCH ANDRE
ROGAWAY PHILLIP WALDER**

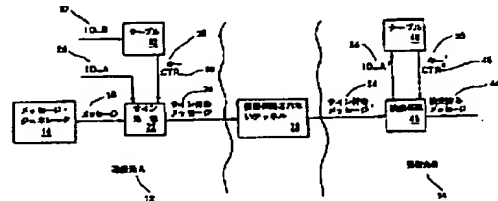
(54) METHOD AND DEVICE FOR DATA AUTHENTICATION IN DATA COMMUNICATION ENVIRONMENT

(57) Abstract:

PURPOSE: To obtain an improved data processing system by generating a tag by combining plural cryptographic words and deciding an authentication tag used with data transfer in which a communication channel is used.

CONSTITUTION: A message is signed by a transmitting origin 12 by a sign processing 22. A message 18, a transmitting origin identifier 26, a shared key 28 and a counter 30 are received by the processing 22. A message 24 with a signature is transmitted with a channel 20. A message 34 is received and an identifier 36 of a signer is extracted by inspecting the message 34 by a receiving destination 14. A value of the receiving destination itself of a key 38 of the receiving destination itself shared by a person who is provided with the identifier equal to the identifier 36 and a value of the receiving destination itself of a CTR 45 is looked up by using the identifier 36 by using a table 42 indexed by the identifier 36 by the receiving destination. After that, the message 34, the identifier 36, the key 38 and the CRT 45 are taken, inspection completion message 44 is recovered or the message 34 is judged to be forged by an inspection processing 43 and when the message 34 is judged to be forged, the message is discarded.

COPYRIGHT: (C)1994,JPO



(19)日本国特許庁(JP)

(12)公開特許公報(A)

(11)特許出願公開番号

特開平6-315027

(43)公開日 平成6年(1994)11月8日

(51)Int.Cl. ⁵	識別記号	庁内整理番号	FI	技術表示箇所
H 0 4 L 9/06				
9/14				
G 0 9 C 1/00		8837-5L		
		8949-5K	H 0 4 L 9/02	Z

審査請求 有 請求項の数44 O L (全 19 頁)

(21)出願番号 特願平6-49081

(22)出願日 平成6年(1994)3月18日

(31)優先権主張番号 0 5 2 3 0 4

(32)優先日 1993年4月23日

(33)優先権主張国 米国(US)

(71)出願人 390009531

インターナショナル・ビジネス・マシーンズ・コーポレーション

INTERNATIONAL BUSINESS MACHINES CORPORATION

アメリカ合衆国10504、ニューヨーク州アーモンク (番地なし)

(72)発明者 ミヒル・ベラーレ

アメリカ合衆国10025 ニューヨーク州ニューヨーク セントラル・パーク・ウェスト372 ナンバー16イー

(74)代理人 弁理士 合田 深 (外2名)

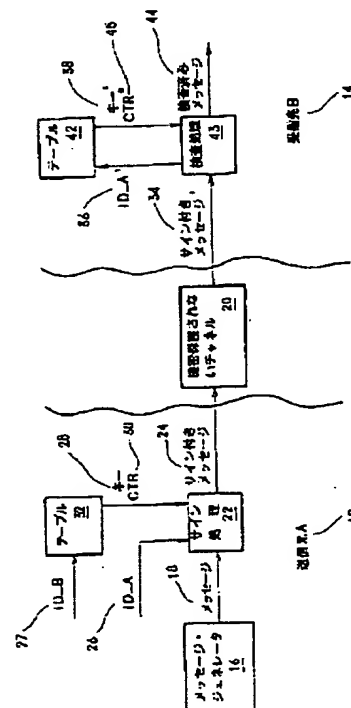
最終頁に続く

(54)【発明の名称】 データ通信環境におけるデータ認証のための方法および装置

(57)【要約】

【目的】 データ通信環境内で、単純、高速かつ安全にデータ認証を提供するためのシステムおよび方法を提供すること。

【構成】 転送するデータ・メッセージを、データ・ブロックに分割する。各データ・ブロックをブロック・インデックスと組み合わせて、ワードを作成する。各ワードに擬似乱数関数を適用して、複数の暗号データ列を作成する。送信元の識別子とカウンタ値を含む識別子用ヘッダも、擬似乱数関数を使用して暗号化する。この暗号化されたデータ列とヘッダを論理的に組み合わせて、タグを作成する。特定のワードの暗号化は他のワードと独立に行われるので、各ブロックを他のブロックとは独立に暗号化することができる。したがって、この方法およびシステムは、並列にまたはパイプライン方式で実行でき構成できる。受信側の構成要素またはシステムは、メッセージ信頼性を判定するために送信されたタグと比較することのできる、第2のタグを生成する。



【特許請求の範囲】

【請求項1】データを複数のブロックに区分するステップと、

前記ブロックのそれぞれについて、前記ブロックを符号化して、前記ブロックの値と前記ブロックの識別子との両方を表すワードを作成するステップと、

前記ワードのそれぞれに擬似乱数関数を適用して、複数の暗号ワードを作成するステップと、

前記複数の暗号ワードを組み合わせ、タグを作成するステップとを含む、通信チャネルを使用したデータの転送と共に使用する認証タグを決定するための方法。

【請求項2】前記擬似乱数関数が、データ暗号化標準（DES）アルゴリズムであることを特徴とする、請求項1の方法。

【請求項3】前記ブロックが、固定長であることを特徴とする、請求項1の方法。

【請求項4】前記組み合わせステップが、排他的論理和演算を含むことを特徴とする、請求項1の方法。

【請求項5】前記タグが、切捨てその他の方法によって所与の長さに短縮されることを特徴とする、請求項1の方法。

【請求項6】前記擬似乱数関数が、多段式であることを特徴とする、請求項1の方法。

【請求項7】前記複数のワードが、前記多段式擬似乱数関数に対してパイプライン化されることを特徴とする、請求項6の方法。

【請求項8】前記複数のワードが、前記複数の多段式擬似乱数関数に同時に提示されることを特徴とする、請求項1の方法。

【請求項9】さらに、少なくとも前記タグを前記識別子と組み合わせ、メッセージ認証コード（MAC）を作成するステップを含む、請求項1の方法。

【請求項10】さらに、少なくともデータとメッセージ認証コードとを組み合わせ、データ・パケットを作成するステップを含む、請求項9の方法。

【請求項11】データを複数のブロックに区分するステップと、

前記ブロックのそれぞれについて、前記ブロックを符号化して、前記ブロックの値と前記ブロックの識別子との両方を表すワードを作成するステップと、

（i）前記ワードのそれぞれと（ii）前記データのヘッダとに擬似乱数関数を適用して、複数の暗号ワードを作成するステップと、

前記複数の暗号ワードを組み合わせ、メッセージ認証コード（MAC）を作成するステップとを含む、通信チャネルを使用したデータの転送と共に使用する認証タグを決定するための方法。

【請求項12】前記擬似乱数関数が、データ暗号化標準（DES）アルゴリズムであることを特徴とする、請求項11の方法。

【請求項13】前記ブロックが、固定長であることを特徴とする、請求項11の方法。

【請求項14】前記組み合わせステップが、排他的論理和演算を含むことを特徴とする、請求項11の方法。

【請求項15】前記ヘッダが、識別子とカウンタとを含むことを特徴とする、請求項11の方法。

【請求項16】前記タグが、切捨てによって所与の長さに短縮されることを特徴とする、請求項11の方法。

【請求項17】前記擬似乱数関数が、多段式であることを特徴とする、請求項11の方法。

【請求項18】前記複数のワードが、前記多段式擬似乱数関数に対してパイプライン化されることを特徴とする、請求項17の方法。

【請求項19】前記複数のワードが、前記複数の多段式擬似乱数関数に同時に提示されることを特徴とする、請求項11の方法。

【請求項20】さらに、少なくとも前記タグを前記識別子と組み合わせ、メッセージ認証コード（MAC）を作成するステップを含む、請求項11の方法。

【請求項21】さらに、少なくともデータとメッセージ認証コードとを組み合わせ、データ・パケットを作成するステップを含む、請求項20の方法。

【請求項22】データを複数のブロックに区分するステップと、

前記ブロックのそれぞれについて、前記ブロックを符号化して、前記ブロックの値と前記ブロックの識別子との両方を表すワードを作成するステップと、

前記ワードのそれぞれに擬似乱数関数を適用して、複数の暗号ワードを作成するステップと、

前記複数の暗号ワードを組み合わせ、タグを作成するステップと、

少なくとも前記データと前記タグとを組み合わせ、データ・パケットを作成するステップと、

非機密保護通信チャネルを介して前記データ・パケットを送信するステップと、

データ・パケットを受信するステップと、

データ・パケットを分解して、タグとデータを抽出するステップと、

少なくとも抽出されたデータと局所キーとから第2タグを生成するステップと、

抽出されたタグと第2タグを比較して、データ・パケットのデータ信頼性を判定するステップとを含む、非機密保護通信チャネルを使用してデータを安全に転送するための方法。

【請求項23】データを複数のブロックに区分するステップと、

前記ブロックのそれぞれにブロック識別子を連結して、ワードを作成するステップと、

前記ワードのそれぞれに擬似乱数関数を適用して、複数の暗号ワードを作成するステップと、

前記複数の暗号ワードを組み合わせて、タグを作成するステップとを含む、通信チャネルを使用したデータの転送と共に使用する認証タグを決定するための方法。

【請求項 2 4】前記ブロック識別子が、ブロック・インデックスに基づくことを特徴とする、請求項 2 3 の方法。

【請求項 2 5】前記擬似乱数関数が、多段式であることを特徴とする、請求項 2 3 の方法。

【請求項 2 6】前記複数のワードが、前記多段式擬似乱数関数に対してパイプライン化されることを特徴とする、請求項 2 5 の方法。

【請求項 2 7】データを複数のブロックに区分するステップと、

前記ブロックのそれぞれについて、前記ブロックを符号化して、前記ブロックの値と前記ブロックの識別子との両方を表すワードを作成するステップと、

(i) 前記ワードのそれぞれと (ii) 前記データの識別子とに擬似乱数関数を適用して、複数の暗号ワードを作成するステップと、

前記複数の暗号ワードを組み合わせて、タグを作成するステップと、

少なくともデータとタグとを組み合わせて、データ・パケットを作成するステップと、

非機密保護通信チャネルを介してデータ・パケットを送信するステップと、

データ・パケットを受信するステップと、

受信したデータ・パケットを分解して、受信データと受信タグを抽出するステップと、

少なくとも受信データと局所キーとから局所タグを生成するステップと、

受信タグと局所タグを比較して、受信データ・パケットのデータ信頼性を判定するステップとを含む、非機密保護通信チャネルを使用してデータを安全に転送するための方法。

【請求項 2 8】データを複数のブロックに区分するステップと、

前記ブロックのそれぞれについて、前記ブロックを符号化して、前記ブロックの値と前記ブロックの識別子との両方を表すワードを作成するステップと、

(i) 前記ワードのそれぞれと (ii) 前記データの識別子とに擬似乱数関数を適用して、複数の暗号ワードを作成するステップと、

前記複数の暗号ワードを組み合わせて、タグを作成するステップと、

少なくともデータ、タグ、送信元識別子および時間変動パラメータを組み合わせて、データ・パケットを作成するステップと、

非機密保護通信チャネルを介してデータ・パケットを送信するステップと、

データ・パケットを受信するステップと、

受信データ・パケットを分解して、受信データ、受信タグ、受信送信元識別子および受信時間変動パラメータを抽出するステップと、

少なくとも受信データ、受信送信元識別子、受信時間変動パラメータおよび局所キーから局所タグを生成するステップと、

受信タグと局所タグを比較して、受信データ・パケットのデータ信頼性を判定するステップとを含む、前記非機密保護通信チャネルを使用してデータを安全に転送するための方法。

【請求項 2 9】前記比較ステップが、さらに、前記受信時間変動パラメータを局所時間変動パラメータと比較して、前記データ信頼性をさらに判定するステップを含むことを特徴とする、請求項 2 8 の方法。

【請求項 3 0】前記受信時間変動パラメータが、受信カウンタを含むことを特徴とする、請求項 2 9 の方法。

【請求項 3 1】前記受信時間変動パラメータが、タイム・スタンプを含むことを特徴とする、請求項 2 9 の方法。

【請求項 3 2】前記受信時間変動パラメータが、シーケンス番号を含むことを特徴とする、請求項 2 9 の方法。

【請求項 3 3】データを複数のブロックに区分するステップと、

前記ブロックのそれぞれにブロック識別子を連結して、ワードを作成するステップと、

(i) 前記ワードのそれぞれと (ii) 前記データの識別子とに擬似乱数関数を適用して、複数の暗号ワードを作成するステップと、

前記複数の暗号ワードを組み合わせて、タグを作成するステップとを含む、通信チャネルを使用したデータの転送と共に使用する認証タグを決定するための方法。

【請求項 3 4】受信データ・パケットを分解して、受信データ、受信タグおよび受信時間変動パラメータを抽出するステップと、

少なくとも受信データ、受信時間変動パラメータおよび局所キーから局所タグを生成するステップと、

受信タグと局所タグを比較して、受信データ・パケットのデータ信頼性を判定するステップとを含む、受信データ・パケットの信頼性を判定するための方法。

【請求項 3 5】前記受信時間変動パラメータが、受信カウンタを含むことを特徴とする、請求項 3 4 の方法。

【請求項 3 6】前記受信時間変動パラメータが、タイム・スタンプを含むことを特徴とする、請求項 3 4 の方法。

【請求項 3 7】前記受信時間変動パラメータが、シーケンス番号を含むことを特徴とする、請求項 3 4 の方法。

【請求項 3 8】前記受信データ・パケットが、さらに送信元識別子を含むことを特徴とする、請求項 3 4 の方法。

【請求項 3 9】さらに、前記送信元識別子を使用して、

5

局所テーブルから前記局所キーを取得するステップを含む、請求項38の方法。

【請求項40】データを複数のブロックに区分する手段と、

前記ブロックのそれぞれを符号化して、前記ブロックのそれぞれの値と前記ブロックのそれぞれの識別子との両方を表すワードを作成する手段と、

前記ワードのそれぞれに擬似乱数関数を適用して、複数の暗号ワードを作成する手段と、

前記複数の暗号ワードを組み合わせ、タグを作成する手段とを含む、通信チャネルを使用したデータの転送と共に使用する認証タグを決定するためのシステム。

【請求項41】データを複数のブロックに区分する手段と、

前記ブロックのそれぞれにブロック識別子を組み合わせ、ワードを作成する手段と、

(i) 前記ワードのそれぞれと(ii) 前記データの識別子とに擬似乱数関数を適用して、複数の暗号ワードを作成する手段と、

前記複数の暗号ワードを組み合わせ、タグを作成する手段とを含む、通信チャネルを使用したデータの転送と共に使用する認証タグを決定するためのシステム。

【請求項42】受信データ・パケットを分解して、受信データ、受信タグおよび受信時間変動パラメータを抽出する手段と、

少なくとも受信データ、受信時間変動パラメータおよび局所キーから局所タグを生成する手段と、

受信タグと局所タグを比較して、受信データ・パケットのデータ信頼性を判定する手段とを含む、受信データ・パケットの信頼性を判定するためのシステム。

【請求項43】前記受信データ・パケットが、さらに送信元識別子を含むことを特徴とする、請求項42のシステム。

【請求項44】さらに、前記送信元識別子を使用して、局所テーブルから前記局所キーにアクセスする手段を含む、請求項43のシステム。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、データ通信手順に関し、具体的には、機密保護されない通信媒体を使用する際に認証済みデータを提供するための手順に関する。

【0002】

【従来の技術】通信システムでは、一般に、2人の当事者が、機密保護されないチャネルを介して、一方の当事者が受け取ったメッセージが実際に他方の当事者が作成したものであることを各当事者が確信できる形で通信できることを望む。機密保護されないチャネルとは、第3者が、通信リンクを通過するメッセージ・トラフィックを監視または調査でき、かつ自分自身のメッセージを挿入できるチャネルである。通信中の2人の当事者は、短

6

いランダムな秘密キーを所有している、または取得できると仮定することができる。機密保護されないチャネルを介してこのような通信を達成するために、当技術分野ではさまざまな技法が知られている。たとえば、その技法は、R. ジュメマン (Juememan)、S. マチアス (Matyas)、C. マイヤー (Meyer) の論文 "Message Authentication", IEEE Communications, 1985年9月等に記載されている。既知の技法の1つでは、各当事者が、送ろうとする各メッセージに、メッセージと秘密キーとおそらくは他の引数との関数として計算される、短いメッセージ認証コード (MAC: Message Authentication Code) を付加する。

【0003】このタイプのシステムは、たとえば、ANSIのX9.9標準 (ANSI X9.9, 1982) によって示されるように、当技術分野で既知である。しかし、このシステムには、MACを計算できる速度が、その基礎となる暗号動作を実行できる速度によって制限されるという欠点がある。ANSI X9.9の機構を示す図10に示されるように、この制限は、この機構の逐次式という性質に起因するものである。この機構は、メッセージをブロックに分割し、ブロックを暗号化し、暗号化されたブロックとメッセージの次ブロックの排他的論理和をとり、その結果を暗号化し、すべてのブロックの処理が終わるまでこれを繰り返すことからなっている。したがって、あるブロックを利用するためには、その前のすべてのブロックが指定に従って暗号化され排他的論理和をとられるまで、待機しなければならない。この逐次式処理は、ブロックの到着速度が単一ブロックの処理に必要な時間の逆数より速い、超高速のネットワークで問題になる。このようなネットワークでは、余分のハードウェアを設けても、MACの計算を高速化するには役立たない。というのは、ボトルネックの原因が、暗号プリミティブの計算に要する時間であって、その計算を行うための資源の不足ではないからである。このようなネットワークでは、暗号プリミティブを計算できる速度に合わせて、送信時間を低減化する必要が生じるはずである。したがって、高速ネットワークでの全体的システム・スループットは、このタイプの逐次式メッセージ・タグ計算によって大きな影響を受け、情報転送の効率が低下する可能性がある。

【0004】

【発明が解決しようとする課題】本発明の目的は、改良されたデータ処理システムを提供することである。

【0005】本発明のもう1つの目的は、データ処理システム用の改善されたデータ転送手順を提供することである。

【0006】本発明のもう1つの目的は、非機密保護通信環境でのデータ用の改良された認証システムを提供することである。

【0007】本発明のもう1つの目的は、データ処理シ

システムで転送されるメッセージの認証に使用されるメッセージ認証コードを決定するための、改善された方法を提供することである。

【0008】

【課題を解決するための手段】本発明は、簡単かつ高速でおそらくは安全にメッセージ認証コード(MAC)を計算する方法を提供する。送ろうとするデータを、データ・ブロックに分割し、このデータ・ブロックに連続したインデックス1、2、3、…、nを付ける。各ブロック*i*について、ブロック*i*の内容とインデックス*i*(識別子)を符号化することによってワード*x_i*を作成する。各ワード*x_i*にそれぞれ擬似乱数関数を適用して、暗号ワード*y_i*を作成する。さらに、送信元の識別子とカウンタを符号化することによって、識別子用シーケンス番号*x₀*(ヘッダ)を作成する。識別子用ヘッダ*x₀*に擬似乱数関数を適用して、暗号ヘッダ*y₀*を生成する。これらの暗号ワードと暗号ヘッダを論理的に組み合わせ、タグ*t*を作成する。タグ*t*は、送信元の識別子(ID_A)およびカウンタの値(CTR)と共に、メッセージ認証コードを形成する。好ましい実施例では、擬似乱数関数がデータ暗号化標準(DES)のアルゴリズムであり、ブロック・サイズなどはそれに従って選択される。

【0009】擬似乱数関数はそれぞれのワードに他のワードと独立に適用されるので、擬似乱数関数の計算は、ワード*x_i*ごとに独立に(たとえば並行にまたはパイプライン式に)実行できる。したがって、この方法およびシステムは、並行にまたはパイプライン式に実行でき構成できる。タグのサイズは、メッセージ長と独立である。受信側の構成要素またはシステムは、メッセージの信頼性を判定する際に送信されたタグと比較できる、第2のタグを生成する。

【0010】

【実施例】図1を参照すると、送信元12が、メッセージまたはデータのある受信先14に安全に送信しようと試みている。この送信元および受信先は、コンピュータ、通信カード、交換機または他の計算実体とすることができる。メッセージ・ジェネレータ16が、送信元12用のメッセージを作成している。このメッセージの内容を、機密保護されないチャネル20を介して受信先14に送信しなければならない。メッセージ・ジェネレータ16は、たとえば、通信スタックの下位層実体、上位層アプリケーション実体、音声データまたはビデオ・データの供給源もしくは他のデータ供給源とすることができる。機密保護されないチャネル20は、たとえば、物理的に露出されたワイヤ、光ファイバ・ケーブル、無線LAN、衛星チャネルなどとすることができる。

【0011】受信先14は、送信元12によって送られたと主張されるメッセージが実際にその送信元によって送られたと確認したいと思う。この目的のため、送信元

は、サイン処理22でメッセージにサインする(すなわち、メッセージを認証する)。こうしてメッセージにサインすることで、サイン付きメッセージ24が生じる。サイン処理22は、メッセージ(message)18、送信元の識別子(ID_A)26、送信元と受信先で共用されるキー(key)28、およびカウンタ(CTR)30を受け取る。キーとCTRは、送信元および受信先の識別子に(テーブル32を介し標準技法を使用して)関連付けられ、この両方が以下でさらに説明するタグ計算に使用される。好ましい実施例では、関連するキー28およびCTR30が、テーブル32に記憶され、受信先の識別子であるID_B27によってインデックスされるものとして示されている。この場合、これらの値を、サイン処理22が当技術分野で既知の普通のインデックス技法を使用して獲得することができる。

【0012】サイン付きメッセージ24は、機密保護されないチャネル20を介して送信される。このチャネルのもう一方の端で、あるサイン付きメッセージ'(signed message')34が受信先14によって受信される。このサイン付きメッセージ'34は、サイン付きメッセージ24と同一であってもそうでなくてもよい。たとえば、この伝送に使用される機密保護されないチャネル(channel)20は機密保護されていないので、送信元12が実際にはサイン付きメッセージ24を送信していないのに、サイン付きメッセージ'34が受信される可能性がある。あるいは、侵入者が、サイン付きメッセージのビットをいくつか変更している可能性もある。

【0013】受信先14は、サイン付きメッセージ'34を受信し、そのサイン付きメッセージ'を検査することによって、そこで主張された署名者の識別子ID_A'36を抽出する。受信先は、ID_A'によってインデックスされるテーブル42を使用することにより、ID_A'36を使用して、ID_A'に等しい識別子を有する者と共用する受信先自体のキー'38と、CTR'45の受信先自体の値を表引きする。その後、検査処理43が、サイン付きメッセージ'34、ID_A'36、キー'38およびCTR'45を取り、検査済みメッセージ44を回復するか、あるいはサイン付きメッセージ'34が偽造であると判断する。偽造が検出された場合、そのメッセージは廃棄され、他の適当な処置をとることができる。

【0014】図2に、図1のサイン処理22を詳細に示す。このサイン処理22は、メッセージ18を受け取り、ブロック46で、このメッセージを、送信元の識別子であるID_A26、カウンタの現在値であるCTR30およびタグ48と連結し、あるいはその他の方法で組み合わせ、符号化する。CTR値は、ブロック54で、テーブル32(図1)から読み取られる。タグ計算56については後で図4を参照して説明するが、これは、ブロック60でのテーブル32(図1)からのキー

28の読取りを含む。結果として得られる連結された文字列、Message、ID_A、CTR、Tag 58が、図1のサイン付きメッセージ24である。このサイン付きメッセージに組み合わされたID_A、CTR、Tag部分(すなわち、メッセージ自体を除くすべて)が、図8の符号86に示されるメッセージ認証コード(MAC)である。

【0015】各メッセージのサイン処理のたびに、ブロック62で、カウンタCTRの現在値が増分され、あるいは新しい値に変更される。この値は、ブロック64で

【0016】ここで図3を参照すると、サイン付きメッセージ34が、受信先14に入ってくる。ブロック66でこのメッセージを分解して、それを構成するメッセージ35、ID_A'36、CTR'40およびタグ41を決定する。ブロック47で、ID_A'36を使用してテーブル42(図1)をインデクシングして、局所キーであるキー38を得る。ブロック68で、メッセージ35、ID_A'36、CTR'40およびキー38を使用して、送信元12が図2のタグ48を計算するのに使用したタグ計算56と同じアルゴリズムを使用して、受信先14が、この受信したサイン付きメッセージ34に適したタグ(TAG')70を計算する。ブロック72で、ブロック68で計算したタグ70が受信したタグ41と異なると判定される場合、この受信された送信は真正ではないとみなされ、ブロック74で廃棄される。タグが一致する場合、ブロック73でテーブル42(図1)からCTR'45を読み取った後に、ブロック76で、受信したカウンタCTR'40を受信先自体のカウンタであるCTR'45と比較する。前者のほうが大きい場合、ブロック78でこのメッセージを受け入れ、ブロック80で受信先のカウンタCTR'45をCTR'の値で置き換え、ブロック82でテーブル42(図1)に書き込む。そうでない場合、受信した送信は真正でないといふとみなされ、ブロック74で廃棄される。

【0017】時間変動パラメータCTR'45の重要性は、所与のCTR'値に対してあるメッセージを受け入れた後に、同じCTR'値で追加のメッセージを受け入れないようにすることである。好ましい実施例では、メッセージごとに増分されるカウンタを使用し、CTRの最近の値だけをセーブするだけで、カウンタ値が複製されないようにする。しかし、送信されたメッセージが送信時の順序と異なる順序で受信される場合には、これが問題をもたらす。この問題は、真正であるとみなされたメッセージ上で受信された最大のCTR'値からなるk要素の集合Sを受信先がセーブすることによって解決される。さらに、受信先は、(前に説明したように)値CTR'をセーブする。あるメッセージは、そのCTR'値が

集合Sに含まれるか、あるいはCTR'以下のCTR'値を有する場合に、再生(すなわち真正でない)と判定される。真正のメッセージを受信した時、そのCTR'値を集合Sに追加し、CTR'をその集合の最小要素で置き換え、その後、Sの最小要素をSから取り除く。これによって、複製CTR'値が有効として受け入れられないことが保証される。

【0018】別法として、タイム・スタンプなど他のタイプの時間変動パラメータをカウンタの代わりに使用することもできる。送信元は、前述のCTRの代わりに、その現在時刻TIMEを使用する。受信先は、受信先の現在時刻TIME'からあるデルタ量の範囲内にあり、既に使用された時刻値の集合Sのどの時刻値TIME'とも異なる、TIME'値を受け入れる。時刻値TIME'は、このTIME'値を使用してメッセージが受け入れられる時、この集合Sに入れられる。TIME'値は、受信先の現在時刻TIME'との差がデルタ量を越える時、集合Sから取り除かれる。同様の技法を使用して、ブロック・シーケンス番号を時間変動パラメータとして使用することもできる。

【0019】図4は、当技術分野で既知のデータ暗号化標準(DES)のアルゴリズムに基づく、図2のタグ計算56と図3のタグ計算68の1実施例を示す図である。この暗号化標準は、たとえば、Federal Information Processing Standard (FIPS) Publication 46, National Bureau of Standards, U.S. Department of Commerce, Washington, D.C., 1977年1月に記載されている。図4に示した方法に関する前提条件は次のとおりである。第1に、キー28(図1)を使用してメッセージを送る実体が1つだけ存在し、したがって、その識別子ID_A 26(図1)は、単にビット0として扱われる。第2に、キーの下で送られるメッセージは、 2^{62} 個未満である(その後、キーは、手動によりまたは自動的に新しいキーに更新される)。第3に、各メッセージは、長さが 2^{31} 個の32ビット・ワード未満である。キーの下で送ることのできるメッセージの数は、カウンタに許容されるビットの数(好ましい実施例では62ビット)によって決まる。1メッセージ内の32ビット・ワードの数は、 2^{31} を上限とする。というのは、この方式ではビット0がブロック・インデックスの前に付加され、31ビットだけがブロック・インデックス/識別子の記述用に残されるからである。

【0020】さらに具体的に図4を参照すると、メッセージ/データ84は、 $K=32$ ビットの倍数になるように、何らかの標準的な方法で埋め込まれる。この埋込みはデータ処理分野で公知であるので、図4には示さない。メッセージ/データ84は、ある個数NのKビット・ブロックからなるとみなされる。図4には、 $N=3$ ブロック(120、122および124)で $K=32$ ビットの場合のメッセージ/データ84の例が示されてい

る。

【0021】各ブロック識別子の32ビット符号化を、符号88に示す。好ましい実施例では、この符号化の最初のビットが0にセットされ、残りのビットは、当該の各ブロックの整数値 i （ブロック・インデックス）の標準2進符号化である。符号90に M_i と示される、このメッセージの i 番目の32ビット・ブロックを、ブロック92でブロック識別子88の末尾に連結する。その結果得られる N 個の64ビット・ブロック89を、ブロック93で、暗号化標準（DES）のアルゴリズムを使用して、それぞれ暗号化する。それぞれの場合に使用されるキー96は、このタグ計算を行うのが送信元と受信先のどちらであるかに応じて、キー28またはキー38になる。その結果得られる N 個の暗号テキスト99のすべてが、ブロック98で、もう1つの暗号テキスト102と共に、ビットごとに排他的論理和をとられる。この追加の暗号テキスト102は、下記のようにして生成される。

【0022】追加の暗号テキスト102は、カウンタ104をワードの下位62ビットに2進符号化することによって形成される。このカウンタ（このタグ計算を実行するのが送信元と受信先のどちらであるかに応じて、図1のCTR30またはCTR'40）の前に、ビット'1'（最上位ビット位置）と送信元の識別子（この動作が送信元と受信先のどちらで発生するのかに応じてID_AまたはID_A'になり、好ましい実施例では1ビット長と仮定される）を連結したものが付加される。最上位ビット群の先頭ビットは、送信元のID/CTRを符号化するワードの空間を、メッセージ・ブロックを符号化する空間から分離するためのものである。最上位から2番目のビットは、送信元の識別子を示すためのものである。空間の分離によって、復号部分が、カウンタ・ブロックとメッセージ・ブロックを識別し、これらを区別できるようになる。というのは、前者は必ずビット1で始まり、後者は必ずビット0で始まるので、これらの組は決して共通要素をもたないからである。その結果得られる64ビット・ワード91は、ブロック110で暗号化基準のアルゴリズムを使用して暗号化される。この暗号テキスト102と他の N 個の暗号テキスト99の排他的論理和をとった後に、その結果得られる64ビット文字列を、ブロック112でより少ないビット数に切り捨てる。図では32ビットに切り捨てられている。もちろん、この切捨ては、代替実施例ではブロック98の排他的論理和の前に行うことができる。その結果得られるタグ114は、このタグ計算を実行するのが送信元と受信先のどちらであるかに応じて、図2のタグ48または図3のタグ'70になる。

【0023】上で説明した方法の多くを変更して、簡単に下記のものを含む代替実施例を得ることができる。

・別個の番号を有するブロックが異なる符号化を引き起

こす限り、ブロック識別子88と符号90で示される32ビット・ブロックからなるメッセージ・ブロックをどのように符号化してもよい。

・R. リヴェスト（Rivest）等の論文“The MD5 Message-Digest Algorithm”, Network Working Group RFC 1321, 1992年4月に記載のハッシュ関数である、MD5に基づく擬似乱数関数など、他の機構をDESの代わりに使用することができる。擬似乱数関数は、当技術分野で一般に知られており、たとえば、O. ゴールドライヒ（Goldreich）、S. ゴールドヴァッサー（Goldwasser）、S. ミカリ（Micali）の論文“How to Construct Random Functions”, Journal of the Association for Computing Machinery, Vol. 33, No. 4, 1986年10月、782-807ページに記載されている。

・ID106とカウンタ（CTR）104の符号化は、そのID/CTR符号化が、番号付きメッセージ・ブロックの符号化空間と異なる空間に含まれる限り、すなわちすべての i 、 m に関して $\langle ID_A, CTR \rangle < i, m \rangle$ と等しくない限り、変更することができる。

・共用キーの下でデータを送信する実体のグループの各メンバにID106によって名前を付けるのに十分なビット数を使用しなければならない。たとえば、2つの実体が共用キーを使用して互いにメッセージを送ろうとする場合、1ビットで十分であり、2つの実体の一方が“0”という名前になり、他方が“1”という名前になる。

【0024】パイプライン化も、上記の技法に簡単に適合させることができる。一部のDESエンジンは、複数の内部的に刻時される段を有し、暗号化アルゴリズムを実行する時に、所与の段のデータが後続の段に転送される。ワードは互いに独立に暗号化できるので、パイプライン式暗号化手法が可能である。ここで図5を参照すると、単一の多段DESエンジンが示されている。このDESエンジンは、図5では、破線で示した4つの段を有する。たとえば、各段は、4ラウンドのDES計算を含むことができる。時刻0に、ワード1がDESエンジンに提示され、暗号化処理を受ける。時刻1に、ワード1（W1）がこのDESエンジンの内部の第2段に移り、ワード2（W2）がこのエンジンの第1段に提示される。時刻2には、ワード1がこのDESエンジンの内部の第3段に移り、ワード2が内部の第2段に移り、ワード3（W3）がこのエンジンの第1段に提示される。同様にして時刻3には、ワード1がこのDESエンジンの内部の第4段に移り、ワード2が内部の第3段に移り、ワード3が内部の第2段に移り、ワード4（W4）がこのエンジンの第1段に提示される。最後に、時刻4に、ワード1がDES暗号化を終えてこのエンジンから出、ワード5（W5）がこのエンジンの第1段に提示される。暗号化されるワードはそれぞれ、他のワードの暗号化された値に依存しないので、段間で別個の動作が可能で独立の内部段を有するDESエンジンを使用すると、

独立の暗号化動作をこのパイプライン方式で実行することができる。

【0025】図6は、並列MAC方式を使用して、高速のメッセージ・ジェネレータ16と低速の擬似乱数関数に基づくサイン処理22の間で帯域幅を一致させる方法を示すタイミング図である。図6のタイミングに関して、4つのDESエンジン134、136、138、140が送信元と受信先の両方で使用可能な、図7の実施態様を仮定する。さらに、メッセージ130は、1単位時間毎に32ビット・ワード1個の割合で生成されているが、基礎となるDESエンジンは、4単位時間毎に64ビット・ワード1つの割合でしか暗号化できないと仮定する。このタイミング図では、2つのワードの排他的論理和、ワードの連結、カウンタの増分、カウンタの更新などに必要な時間を無視しているが、それらの時間は、一般に、暗号化動作の実行に必要な時間よりはるかに短い。図7の装置は、4つのDESエンジン（134、136、138、140）を使用し、認証されるメッセージの長さとは無関係に、その待ち時間は単一のDESエンジンの待ち時間にすぎない。したがって、この並列化によって、メッセージ長が長い時に、従来の方法に比べて大きなスループットの利益が得られる。

【0026】これから図7に示された装置に関して、図6を詳細に説明する。時刻0に、符号化されたID106（図7）とCTR104が、制御論理機構132によってDESエンジン1（図7の134）に提示される。また、時刻0に、好ましい実施例では64ビットである一時変数T（図7の114）が、全ビット0に初期設定される。暗号テキスト150（図7）は、時刻0+4=4にDESエンジン1（図7の134）から出る（前提の1つとして、前述のようにDES暗号化エンジンに4時間単位を要するものとする）。この時、暗号テキスト150は、ブロック146で移動タグT（図7の114）の現在値と排他的論理和をとられる。

【0027】時刻1に、メッセージ130（図7）のワード1（図7の152）が、図7の制御論理機構132によって符号化され（先に図4に関して説明した符号化）、DESエンジン2（図7の136）に提示され、時刻1+4=5にそこから出る。この時、結果として得られる暗号テキスト152が、ブロック146で、T（図7の144）の現在値と排他的論理和をとられる。

【0028】時刻2に、メッセージのワード2（図7の154）が符号化され、DESエンジン3（図7の138）に提示される。これは時刻2+4=6に出る。この時、結果として得られる暗号テキスト154が、ブロック146で、T（図7の144）の現在値と排他的論理和をとられる。

【0029】時刻3に、メッセージのワード3（図7の156）が符号化され、DESエンジン4（図7の140）に提示される。これは時刻3+4=7に出る。この

時、結果として得られる暗号テキスト156が、ブロック146で、T（図7の144）の現在値と排他的論理和をとられる。

【0030】時刻4に、DESエンジン1（図7の134）は、IDとCTRの符号化を処理し終えたばかりであり、ワード4（図7の158）が準備ができている。このワード4がDESエンジン1（図7の134）に提示され、時刻4+4=8にそこから出る。この時、その暗号テキストが、ブロック146で、T（図7の144）の現在値と排他的論理和をとられる。

【0031】メッセージ130の7つのワードがすべて処理されるまで、この処理が継続する。

【0032】この図では、メッセージの最後のワード（図7に160として示されるワード7）は、時刻7にDESエンジン4（図7の140）に入る。暗号テキスト156は、時刻7+4=11に出る時、ブロック146でT（図7の144）の現在値と排他的論理和をとられる。その結果は、ブロック148で切り捨てられ、あるいはそのまま残されるが、メッセージ130全体のタグ114である。

【0033】図9は、すべて共通のデータ経路またはバス172を介して相互接続された、CPU170、読取専用メモリ（ROM）176、ランダム・アクセス・メモリ（RAM）174、入出力アダプタ178、ユーザ・インターフェース・アダプタ182、通信アダプタ194、認証アダプタ195および表示装置アダプタ196を含む、上記の動作を実行するための、好ましい実施例のデータ処理システム168を示す図である。上記の構成要素がそれぞれ、CPUをバス・マスタとし、特定のアドレス範囲をシステム内の各構成要素専用にするなどの方法を含む、当業者に既知の普通の技法を使用して、共通のバスにアクセスする。当業者に既知の他の普通の技法には、DASD180やネットワーク200などの外部装置からデータ処理システムのランダム・アクセス・メモリ（RAM）174へ高速でデータを転送するのに使用される直接メモリ・アクセス（DMA）が含まれる。図9からわかるように、外部装置であるDASD180は入出力アダプタ178を介し、ネットワーク200は通信アダプタ194を介して、共通のバス172にインターフェースする。表示装置198など他の外部装置も、同様に表示装置アダプタ196を使用して、バス172と表示装置198の間のデータ・フローを実現する。ユーザ・インターフェース手段は、ユーザ・インターフェース・アダプタ182によって提供される。ユーザ・インターフェース・アダプタ182には、ジョイスティック192、マウス186、キーボード184、スピーカ188などが接続されている。これらの装置はそれぞれ周知であり、したがって本明細書では詳細には説明しない。

【0034】図9は、下記のように図1に対応する。図

9のネットワーク200は、機密保護されないチャネル20に対応する。図1の送信元12内の諸機能は、図9のデータ処理システム168と認証アダプタ195によって提供される。認証アダプタ195は、図7に示した論理機構および対応する回路を含む。代替実施例では、認証アダプタ195を通信アダプタ194と組み合わせて、さらに性能を高めることができる。図1の受信先14内の諸機能は、図9のデータ処理システム168と同一タイプまたは異なるタイプの別のデータ・プロセッサによって提供される。

【0035】以下のように発明を開示する。

(1) データを複数のブロックに区分するステップと、前記ブロックのそれぞれについて、前記ブロックを符号化して、前記ブロックの値と前記ブロックの識別子との両方を表すワードを作成するステップと、前記ワードのそれぞれに擬似乱数関数を適用して、複数の暗号ワードを作成するステップと、前記複数の暗号ワードを組み合わせ、タグを作成するステップとを含む、通信チャネルを使用したデータの転送と共に使用する認証タグを決定するための方法。

【0036】(2) 前記擬似乱数関数が、データ暗号化標準(DES)アルゴリズムであることを特徴とする、(1)の方法。

【0037】(3) 前記ブロックが、固定長であることを特徴とする、(1)の方法。

【0038】(4) 前記組み合わせステップが、排他的論理和演算を含むことを特徴とする、(1)の方法。

【0039】(5) 前記タグが、切捨てによって所与の長さに短縮されることを特徴とする、(1)の方法。

【0040】(6) 前記擬似乱数関数が、多段式であることを特徴とする、(1)の方法。

【0041】(7) 前記複数のワードが、前記多段式擬似乱数関数に対してパイプライン化されることを特徴とする、(6)の方法。

【0042】(8) 前記複数のワードが、前記複数の多段式擬似乱数関数に同時に提示されることを特徴とする、(1)の方法。

【0043】(9) さらに、少なくとも前記タグを前記識別子と組み合わせ、メッセージ認証コード(MAC)を作成するステップを含む、(1)の方法。

【0044】(10) さらに、少なくともデータとメッセージ認証コードとを組み合わせ、データ・パケットを作成するステップを含む、(9)の方法。

【0045】(11) データを複数のブロックに区分するステップと、前記ブロックのそれぞれについて、前記ブロックを符号化して、前記ブロックの値と前記ブロックの識別子との両方を表すワードを作成するステップと、(i) 前記ワードのそれぞれと(ii) 前記データのヘッダとに擬似乱数関数を適用して、複数の暗号ワード

を作成するステップと、前記複数の暗号ワードを組み合わせ、メッセージ認証コード(MAC)を作成するステップとを含む、通信チャネルを使用したデータの転送と共に使用する認証タグを決定するための方法。

【0046】(12) 前記擬似乱数関数が、データ暗号化標準(DES)アルゴリズムであることを特徴とする、(11)の方法。

【0047】(13) 前記ブロックが、固定長であることを特徴とする、(11)の方法。

10 【0048】(14) 前記組み合わせステップが、排他的論理和演算を含むことを特徴とする、(11)の方法。

【0049】(15) 前記ヘッダが、識別子とカウンタとを含むことを特徴とする、(11)の方法。

【0050】(16) 前記タグが、切捨てによって所与の長さに短縮されることを特徴とする、(11)の方法。

【0051】(17) 前記擬似乱数関数が、多段式であることを特徴とする、(11)の方法。

20 【0052】(18) 前記複数のワードが、前記多段式擬似乱数関数に対してパイプライン化されることを特徴とする、(17)の方法。

【0053】(19) 前記複数のワードが、前記複数の多段式擬似乱数関数に同時に提示されることを特徴とする、(11)の方法。

【0054】(20) さらに、少なくとも前記タグを前記識別子と組み合わせ、メッセージ認証コード(MAC)を作成するステップを含む、(11)の方法。

30 【0055】(21) さらに、少なくともデータとメッセージ認証コードとを組み合わせ、データ・パケットを作成するステップを含む、(20)の方法。

【0056】(22) データを複数のブロックに区分するステップと、前記ブロックのそれぞれについて、前記ブロックを符号化して、前記ブロックの値と前記ブロックの識別子との両方を表すワードを作成するステップと、前記ワードのそれぞれに擬似乱数関数を適用して、複数の暗号ワードを作成するステップと、前記複数の暗号ワードを組み合わせ、タグを作成するステップと、少なくとも前記データと前記タグとを組み合わせ、データ・パケットを作成するステップと、非機密保護通信チャネルを介して前記データ・パケットを送信するステップと、データ・パケットを受信するステップと、データ・パケットを分解して、タグとデータを抽出するステップと、少なくとも抽出されたデータと局所キーとから第2タグを生成するステップと、抽出されたタグと第2タグを比較して、データ・パケットのデータ信頼性を判定するステップとを含む、非機密保護通信チャネルを使用してデータを安全に転送するための方法。

【0057】(23) データを複数のブロックに区分するステップと、前記ブロックのそれぞれにブロック識別

子を連結して、ワードを作成するステップと、前記ワードのそれぞれに擬似乱数関数を適用して、複数の暗号ワードを作成するステップと、前記複数の暗号ワードを組み合わせて、タグを作成するステップとを含む、通信チャネルを使用したデータの転送と共に使用する認証タグを決定するための方法。

【0058】(24) 前記ブロック識別子が、ブロック・インデックスに基づくことを特徴とする、(23)の方法。

【0059】(25) 前記擬似乱数関数が、多段式であることを特徴とする、(23)の方法。

【0060】(26) 前記複数のワードが、前記多段式擬似乱数関数に対してパイプライン化されることを特徴とする、(25)の方法。

【0061】(27) データを複数のブロックに区分するステップと、前記ブロックのそれぞれについて、前記ブロックを符号化して、前記ブロックの値と前記ブロックの識別子との両方を表すワードを作成するステップと、(i) 前記ワードのそれぞれと(ii) 前記データの識別子とに擬似乱数関数を適用して、複数の暗号ワードを作成するステップと、前記複数の暗号ワードを組み合わせ、タグを作成するステップと、少なくともデータとタグとを組み合わせ、データ・パケットを作成するステップと、非機密保護通信チャネルを介してデータ・パケットを送信するステップと、データ・パケットを受信するステップと、受信したデータ・パケットを分解して、受信データと受信タグを抽出するステップと、少なくとも受信データと局所キーとから局所タグを生成するステップと、受信タグと局所タグを比較して、受信データ・パケットのデータ信頼性を判定するステップとを含む、非機密保護通信チャネルを使用してデータを安全に転送するための方法。

【0062】(28) データを複数のブロックに区分するステップと、前記ブロックのそれぞれについて、前記ブロックを符号化して、前記ブロックの値と前記ブロックの識別子との両方を表すワードを作成するステップと、(i) 前記ワードのそれぞれと(ii) 前記データの識別子とに擬似乱数関数を適用して、複数の暗号ワードを作成するステップと、前記複数の暗号ワードを組み合わせ、タグを作成するステップと、少なくともデータ、タグ、送信元識別子および時間変動パラメータを組み合わせ、データ・パケットを作成するステップと、非機密保護通信チャネルを介してデータ・パケットを送信するステップと、データ・パケットを受信するステップと、受信データ・パケットを分解して、受信データ、受信タグ、受信送信元識別子および受信時間変動パラメータを抽出するステップと、少なくとも受信データ、受信送信元識別子、受信時間変動パラメータおよび局所キーから局所タグを生成するステップと、受信タグと局所タグを比較して、受信データ・パケットのデータ信頼性

を判定するステップとを含む、前記非機密保護通信チャネルを使用してデータを安全に転送するための方法。

【0063】(29) 前記比較ステップが、さらに、前記受信時間変動パラメータを局所時間変動パラメータと比較して、前記データ信頼性をさらに判定するステップを含むことを特徴とする、(28)の方法。

【0064】(30) 前記受信時間変動パラメータが、受信カウンタを含むことを特徴とする、(29)の方法。

【0065】(31) 前記受信時間変動パラメータが、タイム・スタンプを含むことを特徴とする、(29)の方法。

【0066】(32) 前記受信時間変動パラメータが、シーケンス番号を含むことを特徴とする、(29)の方法。

【0067】(33) データを複数のブロックに区分するステップと、前記ブロックのそれぞれにブロック識別子を連結して、ワードを作成するステップと、(i) 前記ワードのそれぞれと(ii) 前記データの識別子とに擬似乱数関数を適用して、複数の暗号ワードを作成するステップと、前記複数の暗号ワードを組み合わせ、タグを作成するステップとを含む、通信チャネルを使用したデータの転送と共に使用する認証タグを決定するための方法。

【0068】(34) 受信データ・パケットを分解して、受信データ、受信タグおよび受信時間変動パラメータを抽出するステップと、少なくとも受信データ、受信時間変動パラメータおよび局所キーから局所タグを生成するステップと、受信タグと局所タグを比較して、受信データ・パケットのデータ信頼性を判定するステップとを含む、受信データ・パケットの信頼性を判定するための方法。

【0069】(35) 前記受信時間変動パラメータが、受信カウンタを含むことを特徴とする、(34)の方法。

【0070】(36) 前記受信時間変動パラメータが、タイム・スタンプを含むことを特徴とする、(34)の方法。

【0071】(37) 前記受信時間変動パラメータが、シーケンス番号を含むことを特徴とする、(34)の方法。

【0072】(38) 前記受信データ・パケットが、さらに送信元識別子を含むことを特徴とする、(34)の方法。

【0073】(39) さらに、前記送信元識別子を使用して、局所テーブルから前記局所キーを取得するステップを含む、(38)の方法。

【0074】(40) データを複数のブロックに区分する手段と、前記ブロックのそれぞれを符号化して、前記ブロックのそれぞれの値と前記ブロックのそれぞれの識

別子との両方を表すワードを作成する手段と、前記ワードのそれぞれに擬似乱数関数を適用して、複数の暗号ワードを作成する手段と、前記複数の暗号ワードを組み合わせ、タグを作成する手段とを含む、通信チャネルを使用したデータの転送と共に使用する認証タグを決定するためのシステム。

【0075】(41)データを複数のブロックに区分する手段と、前記ブロックのそれぞれにブロック識別子を組み合わせ、ワードを作成する手段と、(i)前記ワードのそれぞれと(ii)前記データの識別子とに擬似乱数関数を適用して、複数の暗号ワードを作成する手段と、前記複数の暗号ワードを組み合わせ、タグを作成する手段とを含む、通信チャネルを使用したデータの転送と共に使用する認証タグを決定するためのシステム。

【0076】(42)受信データ・パケットを分解して、受信データ、受信タグおよび受信時間変動パラメータを抽出する手段と、少なくとも受信データ、受信時間変動パラメータおよび局所キーから局所タグを生成する手段と、受信タグと局所タグを比較して、受信データ・パケットのデータ信頼性を判定する手段とを含む、受信データ・パケットの信頼性を判定するためのシステム。

【0077】(43)前記受信データ・パケットが、さらに送信元識別子を含むことを特徴とする、(42)のシステム。

【0078】(44)さらに、前記送信元識別子を使用して、局所テーブルから前記局所キーにアクセスする手段を含む、(43)のシステム。

【0079】(45)データを複数のブロックに区分する手段と、前記ブロックのそれぞれを符号化して、前記ブロックのそれぞれの値と前記ブロックのそれぞれの識別子との両方を表すワードを作成する手段と、前記ワードのそれぞれに擬似乱数関数を適用して、複数の暗号ワードを作成する手段と、前記複数の暗号ワードを組み合わせ、タグを作成する手段とを含む、コンピュータ互換媒体上に常駐する、通信チャネルを使用したデータの転送と共に使用する認証タグをデータ処理システムが決定できるようにするためのコンピュータ・プログラム。

【0080】(46)データを複数のブロックに区分する手段と、前記ブロックのそれぞれにブロック識別子を組み合わせ、ワードを作成する手段と、(i)前記ワードのそれぞれと(ii)前記データの識別子とに擬似乱数関数を適用して、複数の暗号ワードを作成する手段と、前記複数の暗号ワードを組み合わせ、タグを作成する手段とを含む、コンピュータ互換媒体上に常駐する、通信チャネルを使用したデータの転送と共に使用する認証タグをデータ処理システムが決定できるようにするためのコンピュータ・プログラム。

【0081】(47)受信データ・パケットを分解して、受信データ、受信タグおよび受信時間変動パラメータを抽出する手段と、少なくとも受信データ、受信時間

変動パラメータおよび局所キーから局所タグを生成する手段と、受信タグと局所タグを比較して、受信データ・パケットのデータ信頼性を判定する手段とを含む、コンピュータ互換媒体上に常駐する、受信データ・パケットの信頼性をデータ処理システムが判定できるようにするためのコンピュータ・プログラム。

【0082】

【発明の効果】本発明により、簡単、高速かつ安全にメッセージ認証コード(MAC)を計算する方法が提供される。

【図面の簡単な説明】

【図1】送信されたメッセージの保全性を保護するデータ通信システムのシステム全体図である。

【図2】通信媒体を使用して転送されるメッセージにサインするための処理を示す図である。

【図3】受信したメッセージを認証するための処理を示す図である。

【図4】データ処理システム内の送信元または受信先のタグ計算の機能を示す図である。

【図5】パイプライン式に使用される多段式DESエンジンを示す図である。

【図6】データ認証で使用されるタグの計算に関するタイミング図である。

【図7】データ処理システム内の送信元または受信先のMAC計算を物理的に示す図である。

【図8】サイン付きメッセージの構造を示す図である。

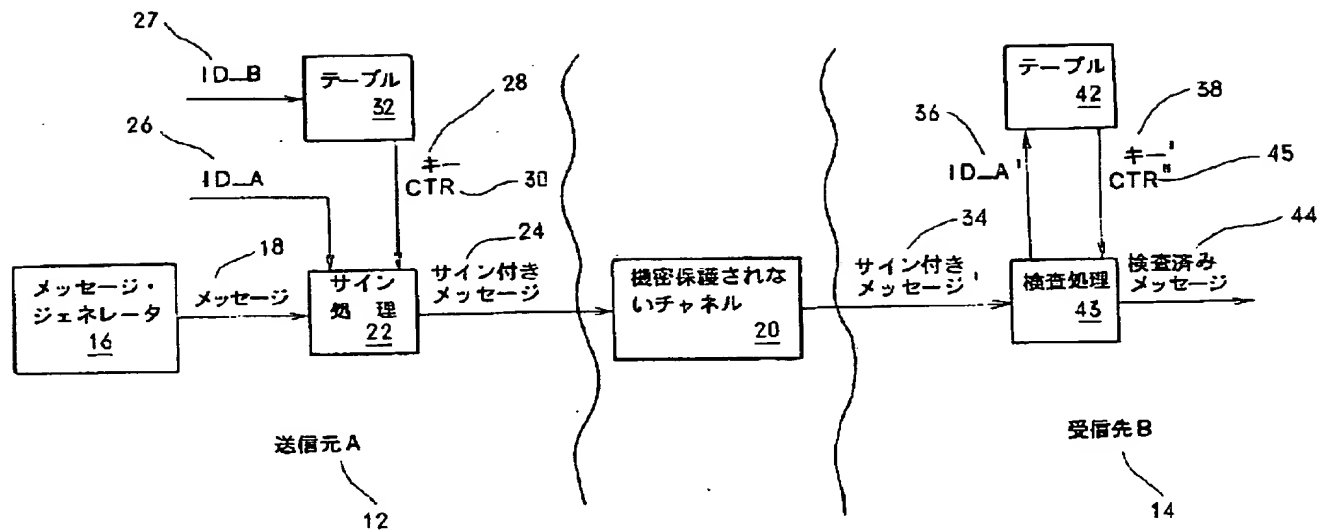
【図9】代表的なデータ処理システムを示す図である。

【図10】逐次式のメッセージ認証コード判定技法を示す図である。

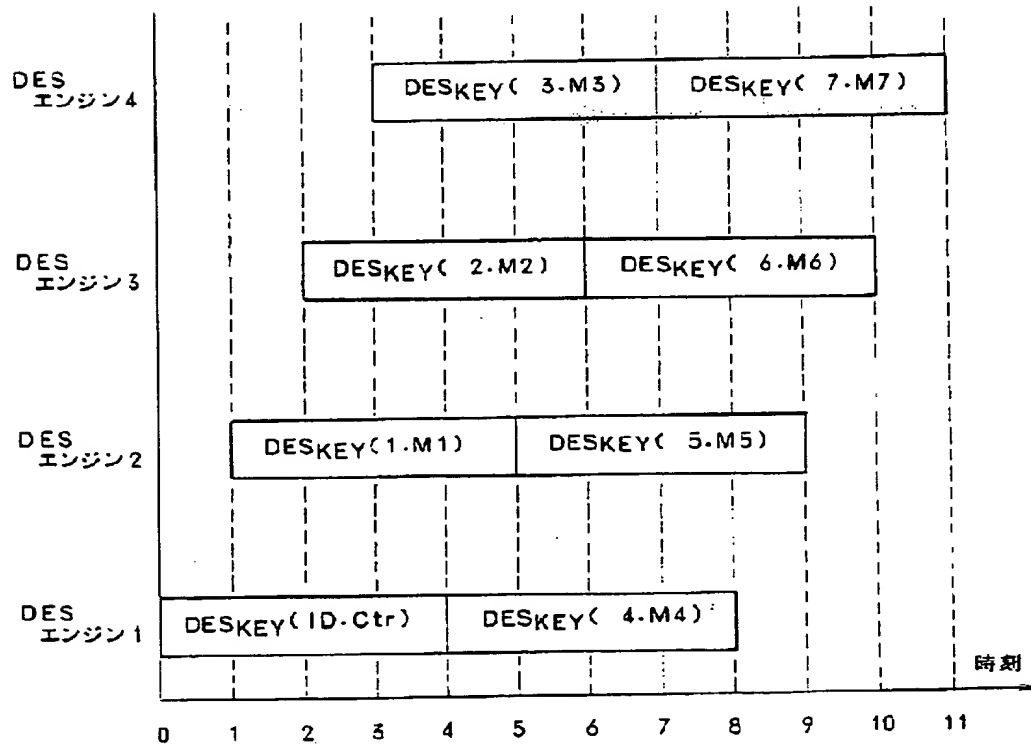
【符号の説明】

- 12 送信元
- 14 受信先
- 16 メッセージ・ジェネレータ
- 18 メッセージ
- 20 機密保護されないチャネル
- 22 サイン処理
- 24 サイン付きメッセージ
- 26 送信元識別子(ID_A)
- 27 受信先識別子(ID_B)
- 28 キー(key)
- 30 カウンタ(CTR)
- 32 テーブル
- 34 サイン付きメッセージ'
- 36 署名者識別子(ID_A')
- 38 キー'(key')
- 40 カウンタ'(CTR')
- 42 テーブル
- 43 検査処理
- 44 検査済みメッセージ

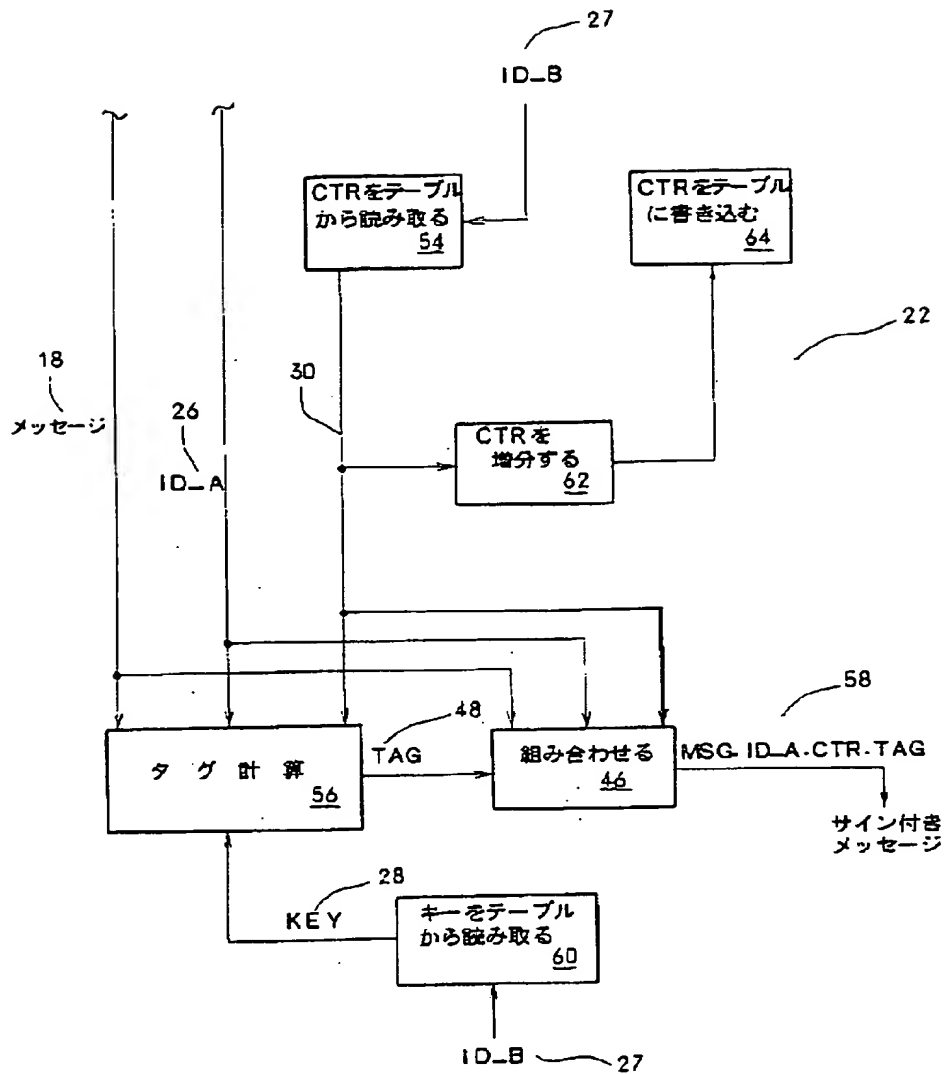
【図1】



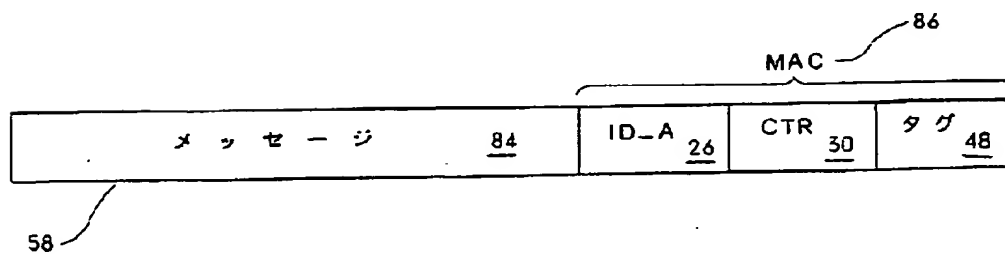
【図6】



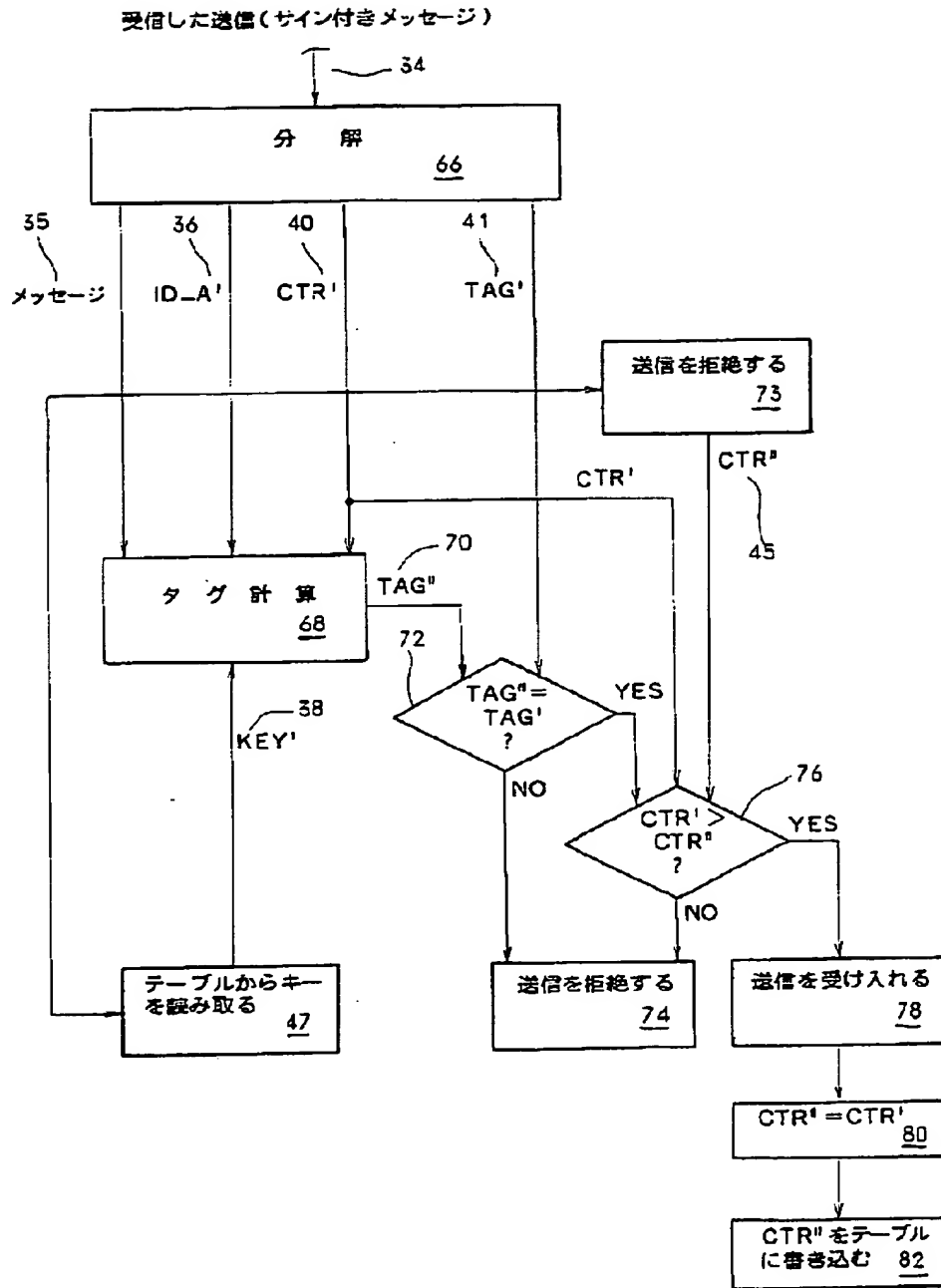
【図2】



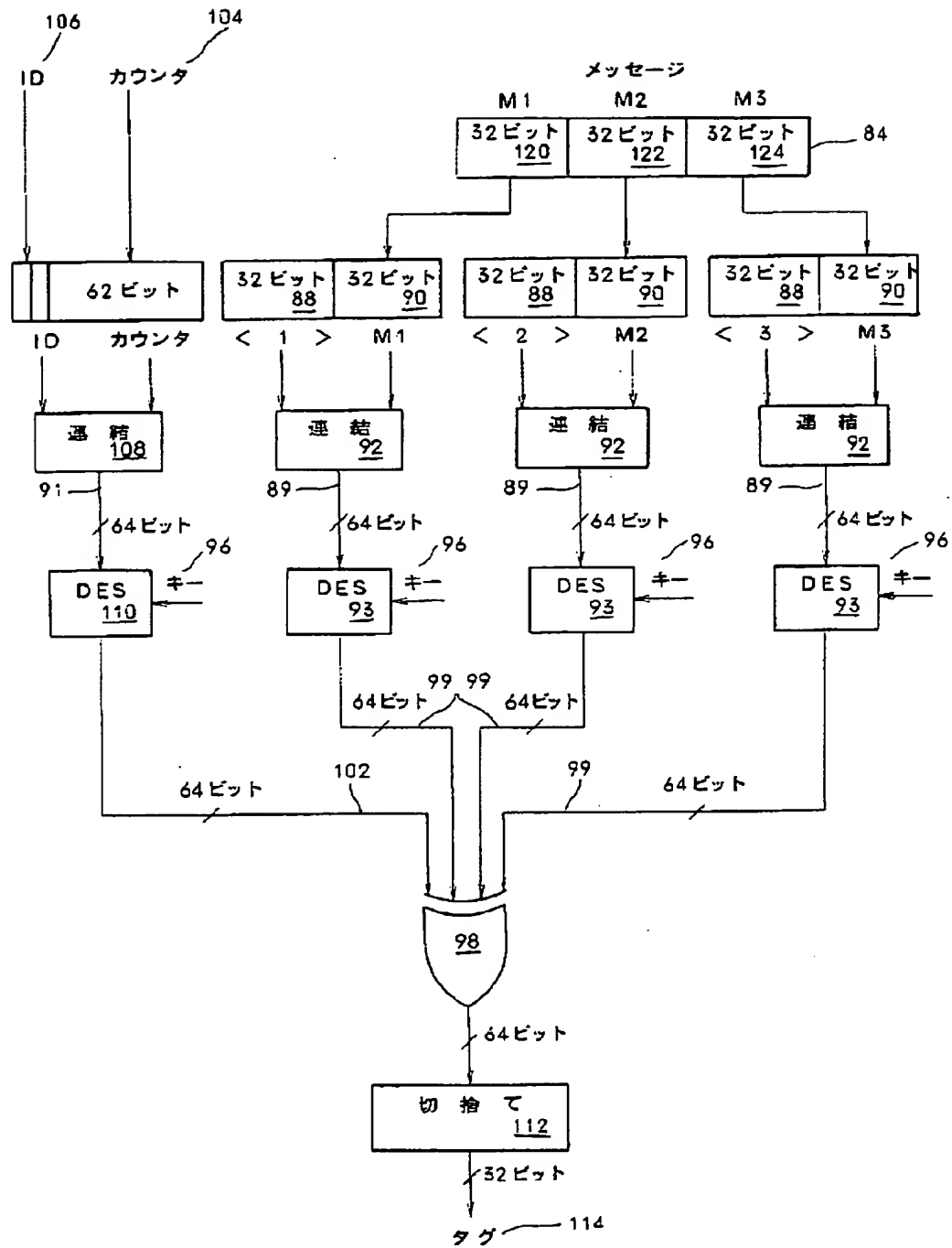
【図8】



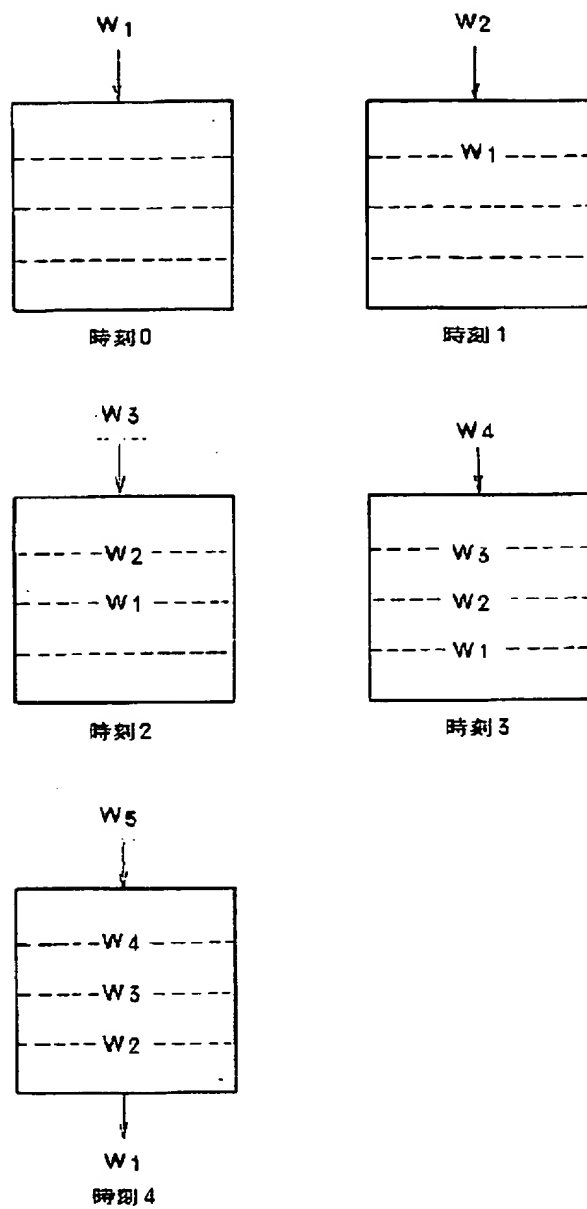
【図 3】



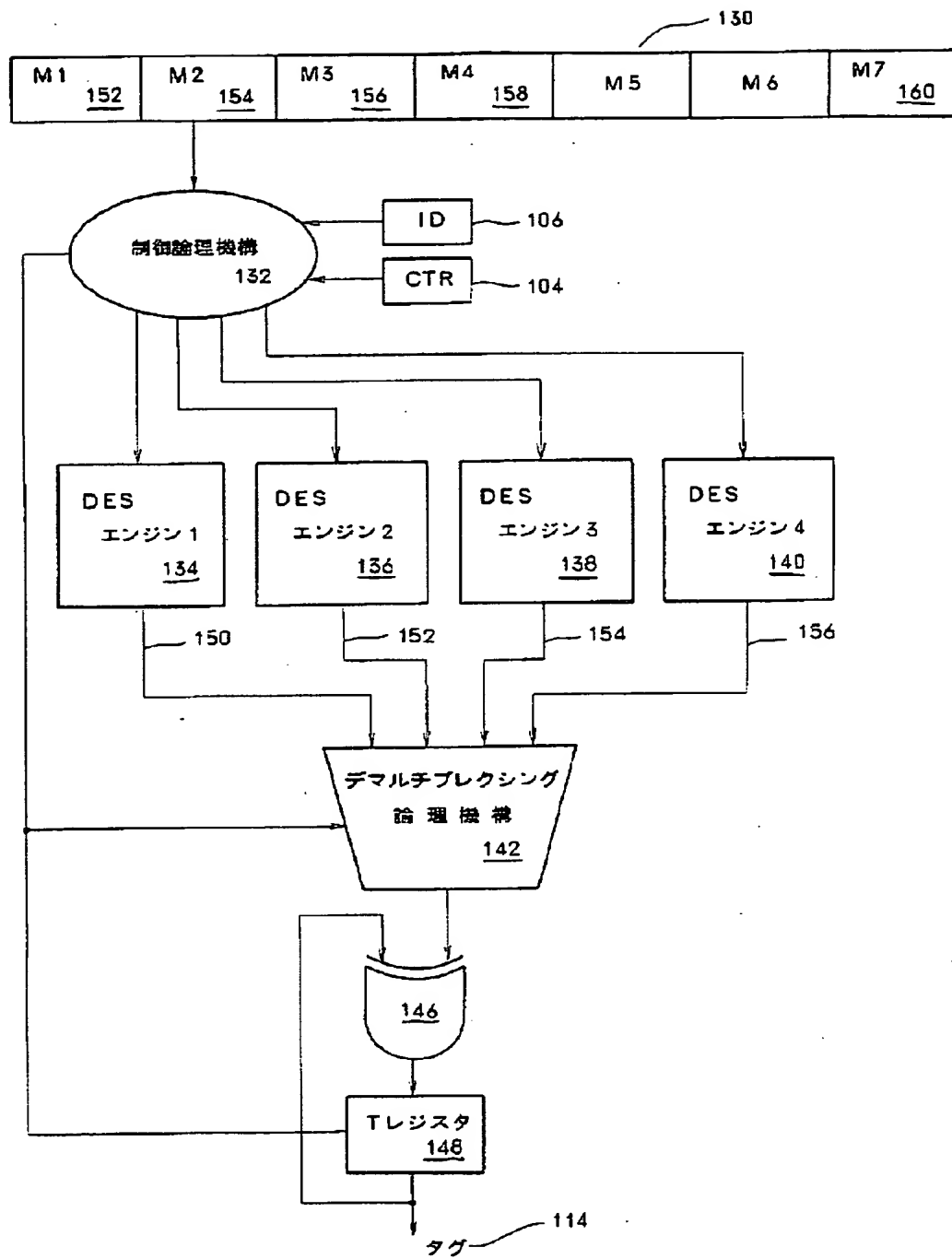
【図4】



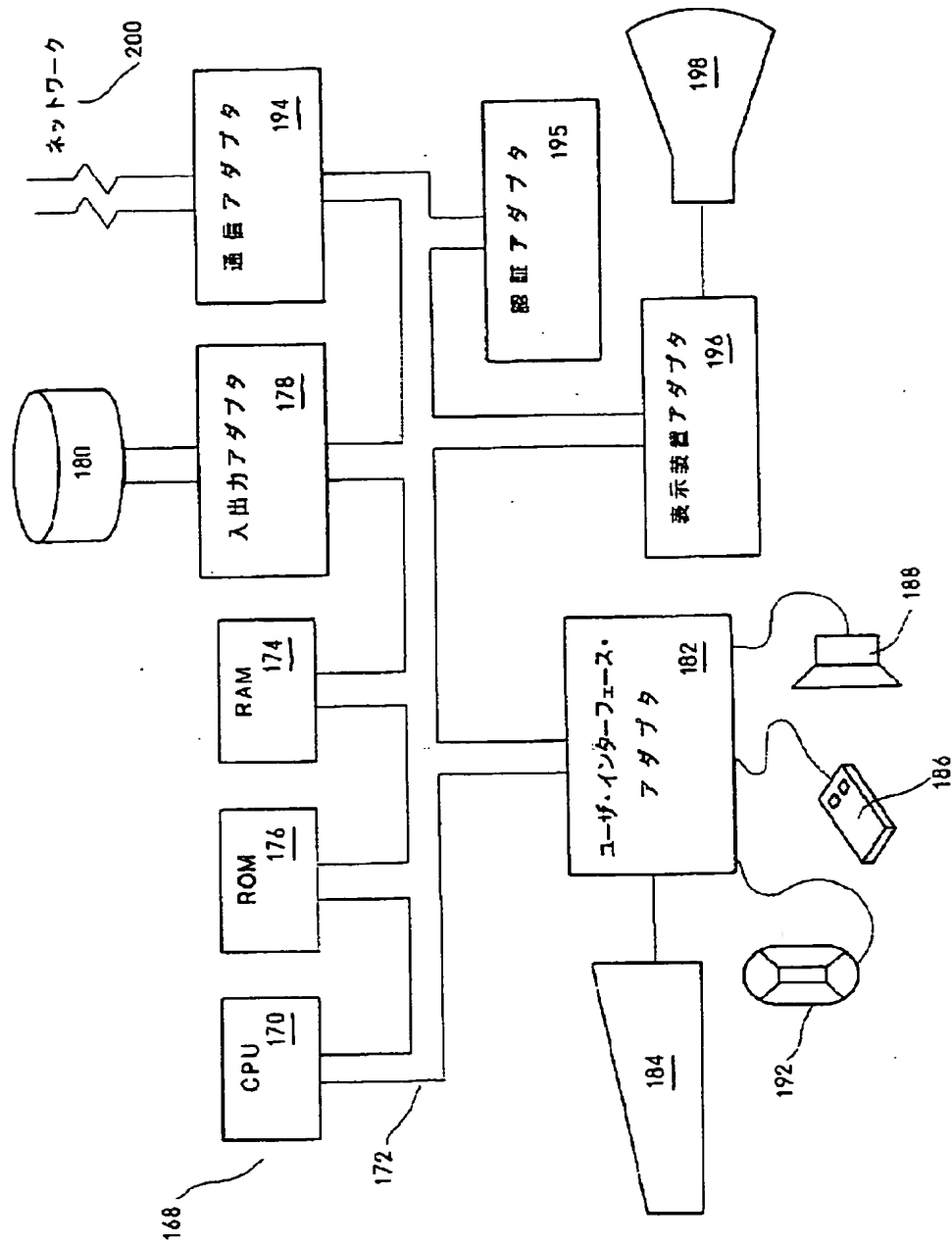
【図5】



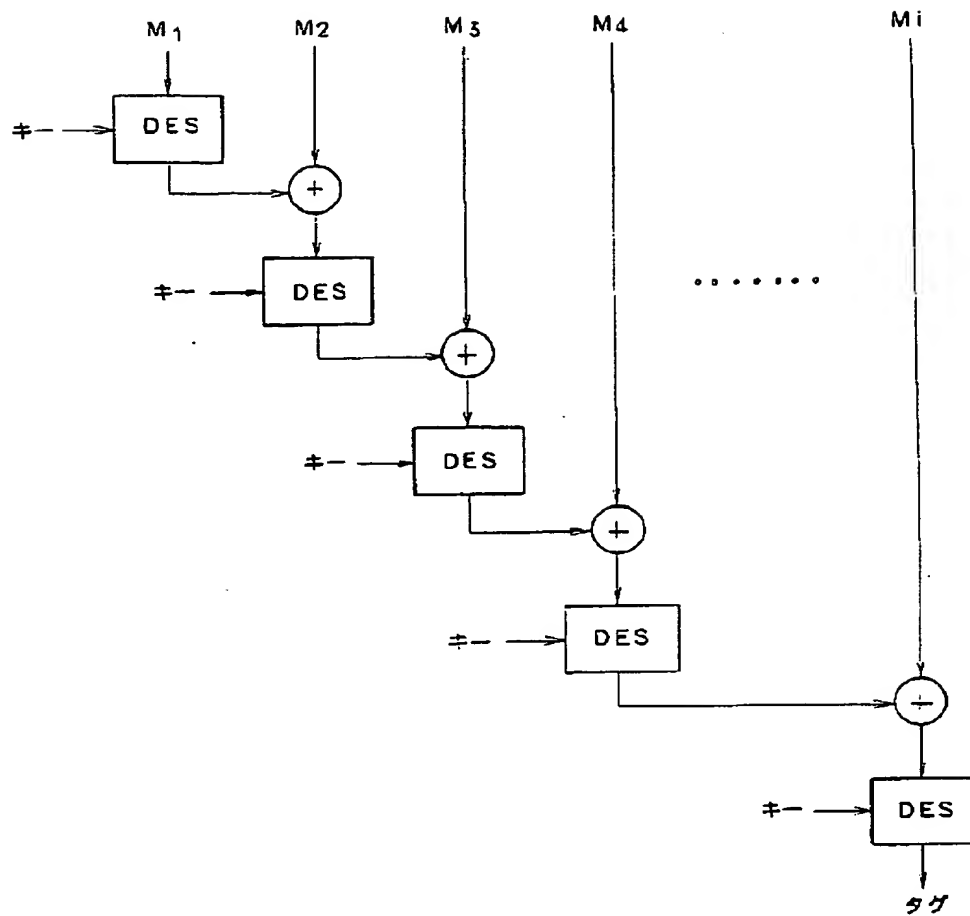
【図 7】



【図9】



【図10】



フロントページの続き

(72) 発明者 ロッシュ・アンドレ・ゲラン
 アメリカ合衆国10598 ニューヨーク州ヨ
 ークタウン・ハイツ ロシャンボー・ドラ
 イブ シーニック・ビュー ナンバー4エ
 イチ

(72) 発明者 フィリップ・ウォルダー・ログウェイ
 アメリカ合衆国78758 テキサス州オース
 チン クリブル・クリーク・ドライブ1620

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☒ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER: _____**

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.